IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings of claims in the application. Please cancel claims 1-14 without prejudice of the subject matter therein. Please add new claims 15-37. No new matter has been added.

1.-14. (Cancelled)

15. (New) A method, comprising:

receiving at a personal identification device a public key;

sending an identifier from the personal identification device to a party based on the public key, the identifier being uniquely associated with the personal identification device; and

receiving at the personal identification device a digital certificate from the party based on the identifier, the personal identification device configured to enroll biometric data after the receiving the public key and after the receiving the digital certificate.

16 (New) The method of claim 15, further comprising sending the public key from the personal identification device to the party after the receiving the public key.

17. (New) The method of claim 15, wherein the receiving the digital certificate from the party is based on the public key and the identifier.

18. (New) The method of claim 15, wherein the identifier is associated with an asymmetric key pair including a personal identification device public key and a personal identification device private key.

19. (New) The method of claim 15, further comprising producing the identifier at the personal identification device.

20. (New) The method of claim 15, further comprising receiving at the personal identification device the identifier from the party.

21. (New) The method of claim 15, wherein the digital certificate includes the public key.

22. (New) The method of claim 15, further comprising:

disabling functionality within the personal identification device until biometric data associated with enrollment is received.

23. (New) A method, comprising:

sending a public key to a personal identification device;

receiving an identifier from the personal identification device, the identifier being uniquely associated with the personal identification device;

producing a digital certificate based on-the identifier; and

sending the digital certificate to the personal identification device such that the personal identification device is configured to enroll biometric data after the receiving the digital certificate.

24. (New) The method of claim 23, wherein the producing of the digital certificate is based, at least in part, on the public key.

25. (New) The method of claim 23, wherein the receiving and the producing is performed by a first party, the method further comprising:

receiving at the first party a digital certificate uniquely associated with a second party different from the first party;

adding a public key of the first party to the digital certificate associated with the second party; and

sending the digital certificate associated with the second party from the first party to the second party.

26. (New) The method of claim 23, wherein the digital certificate includes the public key.

27. (New) The method of claim 23, further comprising producing at the party an asymmetric key pair uniquely associated with the party.

28. (New) An apparatus, comprising:

a memory configured to store biometric data of a user;

a processor coupled to the memory and configured to produce a first identifier based on a public key associated with a first party, the first identifier being uniquely associated with the apparatus;

a biometric sensor coupled to the processor and configured to read biometric input from the user; and

a transmitter coupled to the processor and configured to transmit the first identifier to the first party and a second identifier to a second party different from the first party, the second identifier being uniquely associated with the biometric input.

29. (New) The apparatus of claim 28, wherein the biometric sensor is a fingerprint sensor configured to read a fingerprint from the user.

30. (New) The apparatus of claim 28, wherein the transmitter is a transceiver configured to send information to and receive information from the first party.

31. (New) The apparatus of claim 28, further comprising a receiver configured to receive information from the first party.

32. (New) The apparatus of claim 28, wherein the transmitter is a radio frequency (RF) transmitter.

33. (New) The apparatus of claim 28, further comprising a visual display coupled to the processor.

34. (New) A method, comprising:

receiving an encryption identifier at a personal identification device from a party; and

receiving a digital signature at the personal identification device from the party,

the encryption identifier and the digital signature collectively configured to enable verification of the personal identification device by the party, the personal identification device configured to enroll biometric data after the receiving the encryption identifier and after the receiving the digital signature.

35. (New) The method of claim 34, wherein:

the encryption identifier is a public key; and

the receiving the digital signature including receiving a digital certificate including the digital signature.

36. (New) The method of claim 34, wherein:

the encryption identifier is a public key; and

the receiving the digital signature including receiving a digital certificate including the digital signature based on the public key.

37. (New) The method of claim 34, further comprising:

disabling functionality within the personal identification device until biometric data associated with enrollment is received.